WE CLAIM:

1. A method of implementing a security group within a network, the method comprising:

receiving a packet;

classifying the packet as having a security group designation selected from a plurality of security group designations, the security group designation associating a set of destinations and a set of sources authorized to access the set of destinations; and

applying a security group tag to the packet which identifies the security group designation, the security group tag being applied in a field not reserved for virtual local area network information.

2. The method of claim 1, wherein the security group tag is applied in a field reserved for layer one.

3. The method of claim 1, wherein the security group tag is applied in a field reserved for layer two.

4. A method of implementing a security group within a network, the method comprising:

receiving a packet;

classifying the packet as having a security group designation selected from a plurality of security group designations, the security group designation associating a set of destinations and a set of sources authorized to access the set of destinations; and

applying a security group tag to the packet which identifies the security group designation, the security group tag being applied in a field reserved for security group information.

5. The method of claim 4, wherein the security group tag is applied in a field reserved for layer one.

6. The method of claim 4, wherein the security group tag is applied in a field reserved for layer two.

7. A method for implementing a security group within a network, the method comprising:

receiving a first packet;

classifying the first packet as having a first security group designation selected from a plurality of security group designations, wherein the first security group

designation associates a first set of destinations and a first set of sources authorized to access the first set of destinations; and

applying a first security group tag to the first packet which identifies the first security group designation, wherein the first security group tag is applied in a field reserved for layer three or higher and wherein the information in the field is not used in forwarding decisions by interswitch links.

8. The method of claim 7, further comprising providing authentication information in the first packet.

9. The method of claim 7, further comprising encrypting the first security group tag.

10. The method of claim 7, further comprising:

receiving a second packet;

classifying the second packet as having a second security group designation selected from the plurality of security group designations, wherein the second security group associates a second set of destinations and a second set of sources authorized to access the second set of destinations; and

applying a second security group tag to the packet which identifies the second security group designation.

11. The method of claim 7, wherein the receiving step comprises receiving the packet directly from a source node.

12. The method of claim 7, wherein the classifying step comprises classifying the packet based on a source identity.

13. The method of claim 7, wherein the classifying step comprises classifying the packet based on a payload content.

14. The method of claim 7, further comprising:

(a) receiving a second packet having a second security group tag identifying a particular security group within the enterprise network, wherein the second security group tag is provided in a field of the packet containing layer 3 or higher information, and wherein the field is not used in forwarding decisions by interswitch links;

(b) based on the security group identified in the second security group tag, determining whether to transmit the second packet to its intended destination; and

(c) transmitting the second packet or denying transmission of the second packet to the intended destination based on the determination in (b).

15. The method of claim 10, wherein the second set of sources comprises a source that is included in the first set of sources.

16. The method of claim 10, wherein the second set of destinations comprises a destination that is included in the first set of destinations.

17. The method of claim 12, wherein the source identity comprises a user identity.

18. An apparatus for implementing a security group within a network, the apparatus comprising:

means for receiving a first packet;

means for classifying the first packet as having a first security group designation selected from a plurality of security group designations, wherein the first security group designation associates a first set of destinations and a first set of sources authorized to access the first set of destinations; and

means for applying a first security group tag to the first packet which identifies the first security group designation, wherein the first security group tag is applied in a field reserved for layer three or higher and wherein the information in the field is not used in forwarding decisions by interswitch links.

19. An apparatus for implementing a security group within a network, the apparatus comprising:

a port for receiving a first packet;

a processor for classifying the first packet as having a first security group designation selected from a plurality of security group designations, wherein the first security group designation associates a first set of destinations and a first set of sources authorized to access the first set of destinations; and

an encoder for applying a first security group tag to the first packet which identifies the first security group designation, wherein the first security group tag is applied in a field reserved for layer three or higher and wherein the information in the field is not used in forwarding decisions by interswitch links.

20. A computer program embodied in a computer-readable storage medium, the computer program comprising instructions which cause a computer to:

receive a first packet;

classify the first packet as having a first security group designation selected from a plurality of security group designations, wherein the first security group designation associates a first set of destinations and a first set of sources authorized to access the first set of destinations; and

apply a first security group tag to the first packet which identifies the first security group designation, wherein the first security group tag is applied in a field reserved for layer three or higher and wherein the information in the field is not used in forwarding decisions by interswitch links.

21. A method for implementing a security group within a network, the method comprising:

receiving a packet;

verifying a source of the packet;

reading a destination address of the packet;

reading a security group tag in a field of the packet reserved for layer three or higher;

determining a first security group of the packet based on the security group tag, wherein the first security group is one of a plurality of security groups and wherein the first security group associates a first set of destination addresses and a first set of sources authorized to access the first set of destination addresses; and

deciding, based upon the source and the first security group designation, whether to transmit the packet to the destination address.

22. The method of claim 21, wherein the step of verifying the source of the packet comprises authenticating a source by analyzing authentication information in the packet.

23. The method of claim 21, wherein the step of verifying the source of the packet comprises authenticating a user by analyzing authentication information in the packet.

24. The method of claim 21, further comprising the step of decrypting the packet.

25. The method of claim 21, wherein the first security group is a closed group.

26. The method of claim 21, wherein the first security group is a partially overlapping group.

27. The method of claim 21, further comprising:

receiving a second packet;

classifying the second packet as having a second security group designation selected from a plurality of security group designations, wherein the second security group designation associates a second set of destinations and a second set of sources authorized to access the second set of destinations; and

applying a second security group tag to the second packet which identifies the second security group designation, wherein the second security group tag is applied in a field reserved for layer three or higher and wherein the information in the field is not used in forwarding decisions.

28. The method of claim 21, further comprising the step of applying a policy to the packet based upon the first security group and the destination address, wherein the policy is selected from the group of actions consisting of: forwarding the packet; forwarding the packet and making a record of forwarding the packet; dropping the packet; dropping the packet and making a record of dropping the packet; and inspecting other fields of the packet to determine how to dispose of the packet.

29. A computer program embodied in a computer-readable storage medium, the computer program comprising instructions which cause a computer to:

receive a packet;

verify a source of the packet;

read a destination address of the packet;

read a security group tag in a field of the packet reserved for layer three or higher;

determine a first security group of the packet based on the security group tag, wherein the first security group is one of a plurality of security groups and wherein the first security group associates a first set of destination addresses and a first set of sources authorized to access the first set of destination addresses; and

decide, based upon the source and the first security group designation, whether to transmit the packet to the destination address.

30. An apparatus for implementing a security group within a network, the apparatus comprising:

means for receiving a packet;

means for verifying a source of the packet;

means for reading a destination address of the packet and for reading a security group tag in a field of the packet reserved for layer three or higher; and

means for determining a first security group of the packet based on the security group tag, wherein the first security group is one of a plurality of security groups and wherein the first security group associates a first set of destination addresses and a first set of sources authorized to access the first set of destination addresses and for deciding, based upon the source and the first security group designation, whether to transmit the packet to the destination address.

31. An apparatus for implementing a security group within a network, the apparatus comprising:

a port for receiving a packet; and

a processor for:

verifying a source of the packet;

reading a destination address of the packet;

reading a security group tag in a field of the packet reserved for layer three or higher;

determining a first security group of the packet based on the security group tag, wherein the first security group is one of a plurality of security groups and wherein the first security group associates a first set of destination addresses and a first set of sources authorized to access the first set of destination addresses and

deciding, based upon the source and the first security group designation, whether to transmit the packet to the destination address.

32. A method of implementing a security group in an enterprise network having a plurality of security groups, wherein the security groups each include multiple network nodes within the enterprise network, and wherein the network nodes within a security group are subject to rules governing which network nodes they can communicate with, the method comprising:

(a) receiving a packet having a security group tag identifying a particular security group within the enterprise network, wherein the security group tag is provided in a field of the packet containing layer 3 or higher information, and wherein the field is not used in forwarding decisions;

(b) based on the security group identified in the security group tag, determining whether to transmit the packet to its intended destination; and

(c) transmitting the packet or denying transmission or delaying transmission of the packet to the intended destination based on the determination in (b).

33. The method of claim 32, wherein the method is implemented on a router.

34. The method of claim 32, wherein (c) comprises transmitting the packet only if the security group tag has a specified value.

35. The method of claim 32, wherein the router:

(i) resides in a local area network (LAN) of a multi-LAN enterprise network, and

(ii) physically connects, directly, to a host.

36. The method of claim 32, further comprising the step of applying a policy to the packet based upon the security group and the intended destination, wherein the policy is selected from the group of actions consisting of: forwarding the packet; forwarding the packet and making a record of forwarding the packet; dropping the packet; dropping the packet and making a record of dropping the packet; and inspecting other fields of the packet to determine how to dispose of the packet.

37. The method of claim 34, wherein (c) effects a level of service constraint, and wherein different security groups correspond to different levels of service.

38. A computer program embodied in a computer-readable storage medium for implementing a security group in an enterprise network having a plurality of security groups, wherein the security groups each include multiple network nodes within the enterprise network, and wherein the network nodes within a security group are subject to rules governing which network nodes they can communicate with, the computer program comprising instructions which cause a computer to:

(a) receive a packet having a security group tag identifying a particular security group within the enterprise network, wherein the security group tag is provided in a field of the packet containing layer 3 or higher information, and wherein the field is not used in forwarding decisions;

(b) based on the security group identified in the security group tag, determine whether to transmit the packet to its intended destination; and

(c) transmit the packet or deny transmission or delay transmission of the packet to the intended destination, based on the determination in (b).

39. The computer program of claim 38, wherein the computer program is implemented on a router.

40. The computer program of claim 38, wherein (c) comprises transmitting the packet only if the security group tag has a specified value.

41. The computer program of claim 38, wherein the router:

(i) resides in a local area network (LAN) of a multi-LAN enterprise network, and

(ii) physically connects, directly, to a host.

42. The computer program of claim 40, wherein (c) effects a level of service constraint and wherein different security groups correspond to different levels of service.